REMARKS

Applicants request favorable reconsideration and allowance of this application in view of the foregoing amendments and the following remarks.

Claims 1-52, 54, 56, 58 and 60 are pending in this application, with Claims 1, 8, 12, 20, 27, 34, 37, 45, 52, 54, 56 and 58 being independent.

Claim 53, 55, 57 and 59 have been cancelled without prejudice. Claims 1-7, 9-52, 54, 56, 58 and 60 have been amended. Applicant submits that support for the amendments can be found in the original disclosure, and therefore no new matter has been added.

The Abstract has been amended to conform better with proper U.S. practice. No new matter has been added.

Claims 52-59 were objected to under CFR 1.75(c), as being of improper dependent form. Applicants submit that the amended claims are in proper form and request withdrawal of this objection.

Claims 8-9 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants respectfully submit that this rejection was included erroneously. The features mentioned by the Examiner (device manufacturing apparatus and exposure apparatus) do not appear in the present claims.

Claims 52-59 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Applicants have amended the claims to recite a computer-readable medium. Accordingly, Applicants submit that these claims are directed to a product and recite patent-eligible subject matter.

Claims 1-60 were rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent 5,812,671 to Ross, Jr. in view of European Patent No. 1 045 386 A1 to Herpel et al. Applicants respectfully traverse this rejection for the reasons discussed below.

As recited in independent Claim 1, the present invention includes, *inter alia*, the features of encoding a digital signal with a first encryption key, encoding the first encryption key with a second encryption key associated with a destination server device, and transferring the encoded digital signal and the encoded first encryption key to the destination device. With these features, security of the digital signal can be maintained effectively, yet encryption and transfer to various

destinations can be managed easily. In particular, only the destination server device has the second encryption key to be able to decrypt the encoded signal and, when sending the encoded signal to multiple destinations, it is only necessary to change the encryption of the first encryption key by using different second encryption keys, which is quicker than re-encrypting the whole signal.

Applicants submit that the cited art fails to disclose or suggest at least the above-mentioned features of Claim 1, and therefore it fails to provide the advantages resulting from those features. Ross discloses a cryptographic system for data transmission over a public network, and more particularly to a system which allows parties to send encrypted data messages to one another without key transfer between the parties and without reference to the receiving parties' encryption / decryption protocol (column 1 lines 7 to 12). Figure 1 depicts a cryptographic communications system including a node A having application programs for encryption / decryption 12 and a suitable network interface program 14 for coupling the node to a network 16. **Ross discloses at** column 2, lines 40 to 52 that the choice of an encryption algorithm in node A is independent of the decryption algorithm used by the intended recipients of node A's encrypted message. When node A sends an encrypted file to node B over the network 16, encryption application program 12 encrypts a clear text file using node A's algorithm and secret key 20.

The cryptographic communications system of figure 1 further comprises an encryption gateway 22 including a network interface 24, a decryption server 26, an encryption server 28 and an encryption /decryption manager 30. The encryption/decryption program for implementing the encryption/decryption algorithm for each node and the current key for each node recognized by the encryption gateway are stored in files 32 and 34, respectively, which are accessed by the manager 30. When node A sends its encrypted file to node B over the network 16, this encrypted file is received by the gateway 22 and the manager 30 thereof will fetch node A's decryption algorithm from file store 32 and current key from store 34. The manager 30 loads these files into the decryption server 26, which de-encrypts the incoming encrypted data file.

Further, manager 30 fetches the encryption algorithm and associated key for node B, and loads them into the encryption server 28. Then, encryption server 28 encrypts the plain text file

output of server 26 using node B's algorithm and key. The encrypted message file is then sent to node B. Node B has the same components as node A and decrypts the encrypted message file using node B's decryption algorithm and associated key.

This procedure of encrypting/decrypting a message sent from node A to node B via gateway 22 is fully described on column 2 line 31 to column 3 line 35 with reference to figure 1. Further, the flow chart in figure 2 details the steps performed by the cryptographic communications system depicted in figure 1 (column 3 line 36 to column 4 line 3). In particular, the disclosed steps are:

- encrypting a message in node A using node A's algorithm and key,
- transferring the encoded message to gateway 22,
- in gateway 22, decrypting the encoded message using node A's algorithm and key and re-encrypting the message using node B's algorithm and key, -

sending the re-encrypted message to node B,

- in node B, decrypting the encoded message using node B's algorithm and key.

These steps correspond exactly to the above-mentioned description made with reference to figure 1.

In the Office Action, at page 5, the Examiner considered Ross disclosure's with respect to claim 1 based on the passage mentioned at column 3 lines 35 to 53 with reference to figure 2 and wrote "node A is the client and node B is the destination ... file is transferred to A's network server interface, where a decision can be executed to send the file encrypted . . . " However, as described above, Ross discloses that when encrypting the message to be sent to node B, node A encrypts the message using node A's algorithm and key and sends the encrypted message via gateway 22. There is no indication that node A's key is encoded using another encryption key.

Further, in gateway 22, the encrypted message is decrypted using node A's algorithm and key to obtain a plain message and then re-encrypted using node B's algorithm and key. There is no indication that gateway 22 encrypts node B's key with another encryption key.

Further, as clearly mentioned in Ross at column 1 lines 7 to 12, no key transfer occurs between node A and node B.

Given that neither node A nor gateway discloses encoding a first encryption key with a second encryption key, there is of course no disclosure of sending the encoded first encryption key to a destination server device.

Accordingly, Applicants submit that Ross fails to disclose or suggest at least the above-mentioned features of Claim 1, wherein a digital signal is encoded with a first encryption key, the first encryption key is encoded with a second encryption key associated with a corresponding destination station, and the encoded digital signal and the encoded first encryption key are transferred to a destination server device.

Applicants submit that Herpel fails to remedy the deficiencies of Ross. Herpel is directed to a method for preventing illegal content copies of multimedia content while preserving sufficient flexibility for a legitimate content user. According to Herpel, multimedia content items are accompanied by content descriptors that specify the legitimate rights that are associated to the content item. In the described context, multimedia content in stored on a primary mass storage device. The procedure to transfer a multimedia content item and its associated usage rights, embedded in a content descriptor, from the primary storage device to a secondary storage device are described on column 3 lines 10 to 24. In particular, it is mentioned that the multimedia content item itself as well as the content descriptor are copied to the secondary device.

In case of encrypted or partially encrypted content, the descriptor will contain the decryption key valid for the primary device. Then, the content descriptor on the primary device is removed but not the complete multimedia content item. Finally, a next decryption key for use of the multimedia content item on the secondary device is generated and inserted in the copied content descriptor.

Thus, Herpel likewise fails to disclose or suggest the above-mentioned features of Claim 1. In particular, in Herpel there is no indication that when transferring the encrypted multimedia content item from the primary storage device to the secondary storage device the key used for encrypting this content is also encoded with a second encryption key prior to being sent to the secondary storage device.

For the foregoing reasons, Applicants submit that the present invention recited in independent Claim 1 is patentable over the art of record, whether that art is considered individually or in combination.

The other independent claims recites features similar to those of Claim 1 discussed above, and those other claims are believed patentable for reasons similar to Claim 1.

The dependent claims are patentable for at least the same reasons as the independent claims, as well as for the additional features they recite.

In view of the foregoing, Applicants submit that this application is in condition for allowance. Favorable reconsideration and an early Notice of Allowance are sought.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicants
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/lcw

FCHS_WS 1705243_1.DOC